REMARKS

The above amendments to the above-captioned application along with the following remarks are being submitted as a full and complete response to the Office Action dated November 7, 2005 (U.S. Patent Office Paper No. 20051026) and in connection with the Request for Continued Examination being submitted herewith. In view of the above amendments and the following remarks, the Examiner is respectfully requested to give due reconsideration to this application, to indicate the allowability of the claims, and to pass this case to issue.

Status of the Claims

As outlined above, claims 5-8 are being cancelled without prejudice or disclaimer, and new claim 9 is hereby submitted for consideration to more particularly point out and distinctly claim the subject invention. The support for claim 9 may be found on p. 12, line 8-p.14, line 12. Applicant hereby submits that no new matter is being introduced into the application through the submission of this response.

Prior Art Rejections

First 35 U.S.C. §103(a)rejection

Claims 5 and 8 are rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Matsumoto (Speeding up Secret Computations with Insecure Auxially Devices. Advances in Crytology-Crypto '88, Springer-Verlag Berlin Heidelberg. 1990. pp 497-506). These rejections are respectfully traversed. Note that claims 5-8 are being cancelled and claim 9 is added to more particularly point out and distinctly claim the subject invention.

According to the Manual of Patent Examining Procedure (M.P.E.P. §2143),

> To establish a prima facie case of obviousness, three basis criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both not found in the prior art, not in the applicant's disclosure.

The Office Action contends that Matsumoto discloses a system identical to Applicants' invention except for the use of a third matrix R which further enciphers the original problem and that it would have been obvious to one of ordinary skill in the art at the time of the invention to eliminate the use of the third matrix in Matusmoto's system because it allows for less processing to be done which reduces processing time.

Specifically, the Office Action contends that Applicants disclose that A is a matrix and b is a vector while Matsumoto discloses that both A and B are matrices, however, Matsumoto meets the limitation of the claim with regard to A being a matrix and b being a vector because a vector is a specific kind of a matrix. Further, the Office Action contends that Applicants disclose that P is a nonsingular matrix and Q is a permutation matrix while Matsumoto discloses that both P and Q are permutation matrices, however, Matsumoto meets the limitation of the claim with regard to P being a nonsingular matrix and Q being a permutation matrix because a permutation matrix is a nonsingular matrix. Further, the Office Action specifically contends that Applicants disclose that x and y are subject to inequality constraint $x \geq 0$ while Matsumoto does not discloses that x has to be greater than or equal to 0, however, Matsumoto's system encompasses the inequality constraint $x \geq 0$ because x is open in Matsumoto's system, and therefore meets the limitation of the claim with regard to the inequality constraint. Further, the Office Action contends that Matsumoto's system includes a ciphering key input interface because the client in Matsumoto's system has means for enciphering a problem or a ciphering key, and therefore it is inherent that the client has an interface through which the key was received in the client system. Applicants respectfully disagree for the reasons set forth below.

The present invention recited in new claim 9 provides that a client computer system generating a nonsingular matrix (m x m) and a permutation matrix Q (n x n) using a ciphering key. More precisely, in the present invention, matrices P and Q are generated by using random numbers of a ciphering key. (p. 17, line 8 – p. 20, line 13 of the Specification). In contrast, Matsumoto merely shows that a client randomly generates matrices P and Q (p. 500). Matsumoto says nothing about the use of a ciphering key to generate matrices P and Q. Furthermore, Matsumoto neither expressly nor inherently describes the use of a ciphering key to generate matrix P and Q. Accordingly, it would not have been obvious to a person skilled in the art to create the invention of claim 9.

Second 35 U.S.C. §103(a) rejection

Claims 6 and 7 are rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Matsumoto in view of Kagami (U.S. Pat. No. 5,974,400). The Office Action specifically contends that Matsumoto shows all the steps of a solving service processing method except that it does not teach the steps of sending a program from said server system to said client system in response to a service start request issued by said client system and receiving, in said client system, said program. The Office Action further contends that Kagami shows the steps of sending a program from said server system to said client system in response to a service start request issued by said client system and receiving, in said client system, said program, and that it would have been obvious to one having ordinary skill in the art at the time of invention to incorporate Kagami into Matsumoto in order to support the limitation.

As mentioned above, Claims 6 and 7 are now being canceled and new claim 9 is added to more particularly point out and distinctly claim the subject invention. Claim 9 does not contain the limitation of a step of sending a program from the server system to the client system in response to a service start request issued by the client system. Accordingly, this rejection should be withdrawn.

Furthermore, ass mentioned above, Matsumoto does not show that a client computer system generates matrices P and Q by using a ciphering key. Kagami merely shows that in a server-client communication network, the client inputs and sends a service identifier to the server, receives a program to execute the service from the server, input secret data as a client controlled data from an input device and sends a server control data request to the server and then receives the requested data from the server. Kagami, however, does not show a client computer system generates matrices P and Q by using a ciphering key. Furthermore, Kagami neither expressly nor inherently describes the use of a ciphering key to generate matrices P and Q. Accordingly, it would not have been obvious to a person skilled in the art to create the invention of claim 9.

Conclusion

In view of all the above, Applicants respectfully submit that certain clear and distinct differences as discussed exist between the present invention as now claimed and the prior art references upon which the rejections in the Office Action rely. These differences are more than sufficient that the present invention as now claimed would not have been anticipated nor

rendered obvious given the prior art. Rather, the present invention as a whole is distinguishable, and thereby allowable over the prior art.

Favorable reconsideration of this application as amended is respectfully solicited. Should there be any outstanding issues requiring discussion that would further the prosecution and allowance of the above-captioned application, the Examiner is invited to contact the Applicant's undersigned representative at the address and phone number indicated below.

Respectfully submitted,

Stanley P. Fisher
Registration Number 24,344

Juan Carlos A. Marquez
Registration Number 34,072

REED SMITH LLP
3110 Fairview Park Drive
Suite 1400
Falls Church, Virginia 22042
(703) 641-4200

February 7, 2006
SPF/JCM/YOM